REMARKS

Claims 1-25 were withdrawn from consideration. The Examiner entered a new grounds of rejection for Claims 26-50. Claims 26-50 are now rejected under 35 U.S.C. 102(e) as being anticipated by Brewer (USP 6,922,785).

In the Previous Office Action Response, Applicants argued that Brewer does not teach or suggest any "security control indicator in the frame" or any "security association identifiers associated with the frame" to identify an entry in a "security database."

The Examiner argued that Brewer describes a "type of encryption" flag and the "type of encryption" flag is a security control indicator. This "type of encryption" flag "may be used to indicate an encryption method." The Applicants acknowledge that Brewer does describe a message type field that may be used to indicate an encryption method. However, a type of encryption field that may be used to indicate an encryption method is not a security control indicator. To facilitate prosecution, the independent claims have been amended to recite a security control indicator that is used to "determine if the frame is encrypted and authenticated."

A security control indicator that is used to determine if the frame is encrypted and authenticated is a different type of indicator than a type of encryption flag. The security control indicator also serves a different purpose from an encryption method field. In many instances, an encryption method field provides no information for determining if the frame is encrypted and authenticated. For example, a frame may not be encrypted but may still have the encryption type field in the header to indicate to a switch how to encrypt a frame. In other instances, a frame may have already been decrypted but the type of encryption flag may remain. A switch reading the encryption method field would not be able to obtain any information on whether a frame is encrypted and authenticated based on the encryption method field. That is, a switch can not determine from an encryption method field whether a frame is encrypted or not.

In many instances, a switch may assume that a frame having the encryption method field is encrypted, and this may or may not be a correct assumption. Furthermore, because a security control indicator only has to provided information to determine if the frame is encrypted and authenticated, the security control indicator can be a lot smaller in many examples than an encryption method field. For example, a switch would be able to quickly determine if a frame is

encrypted and authenticated without any knowledge of encryption methodologies. Many bits would not be required to hold the numerous different encryption methodologies available. Furthermore, Brewer does not teach or suggest any mechanism for determining if a frame is authenticated. Brewer only describes a method of encryption field. Encryption does not necessarily entail authentication.

Having a security control indicator allows processing under a standard protocol that does not support encryption. For example, "Figure 10 is a process flow diagram showing a network node in a fibre channel fabric receiving a frame. At 1001, the frame is received. At 1003, it is determined if the frame is secured. Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security. A frame that supports encryption and authentication is herein referred to as a secured frame. A frame that supports only authentication is herein referred to as an authentication secured frame. A frame that supports only encryption is herein referred to as an encryption secured frame."

That is a conventional protocol such as a conventional fibre channel protocol can be used. "If the frame is not secured, processing proceeds using a conventional fibre channel protocol. If the frame is secured, an identifier such as a security parameters identifier SPI is referenced against a security database such as a security association database at 1005. Key information and algorithm information are extracted from the entry containing the identifier or security parameters index associated with the received frame." According to various embodiments, the encryption method is obtained from the security association database. Consequently, Brewer actually indicates that it does not have a security association database because the encryption methodology is included in the encryption methodology field in the header. The network interface card (NIC) of Brewer can then quickly perform decryption using information from the header without having the overhead of accessing any database to determine methodology. This combined with the fact that Brewer does not explicitly describe any security association database suggests that Brewer does not use any security association database as recited in the independent claims.

The statement in the previous Office Action Response "independent claims 26, 36, and 48 do not teach or suggest a variety of elements recited in the independent claims" was intended

to be "portions of Brewer cited to anticipate independent claims 26, 36, and 48 do not teach or suggest a variety of elements recited in the independent claims."

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

/Godfrey Audrey Kwan/
Godfrey Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100